



## DEPARTMENT OF THE NAVY

COMMANDING OFFICER  
NAVAL AIR STATION  
700 AVENGER AVENUE  
LEMOORE, CALIFORNIA 93248-5001

NASLEMINST 5511.2M

10

**FEB 16 2000**

### NAS LEMOORE INSTRUCTION 5511.2M

From: Commanding Officer, Naval Air Station, Lemoore

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM

Ref: (a) SECNAVINST 5510.30A  
(b) SECNAVINST 5510.36  
(c) NASLEMINST 5239.1F  
(d) CINCPACFLT Pearl Harbor HI 220531Z Nov 94  
(e) OPNAVINST 1700.9D  
(f) SECNAVINST 5510.36  
(g) CINCPACFLT Pearl Harbor HI 042333Z Jun 96

Encl: (1) Classified Material Storage Site Listing  
(2) Emergency Plan  
(3) Security Orientation Briefing Guideline  
(4) Photocopier Warning Signs

1. Purpose. To implement subject program following references (a) through (g) and enclosures (1) through (4).

2. Cancellation. NASLEMINST 5511.2L

3. Policy. All classified information, whether written, printed, spoken, photographed, taped, or recorded by other means, shall be protected from unauthorized disclosure. Each individual, military or civilian, assigned or employed by this command is responsible individually for compliance with this instruction and references (a) and (b).

4. Security Management

a. Responsibilities

(1) In addition to the responsibilities as outlined in references (a) and (b), the following guidance applies to Naval Air Station (NAS) Lemoore:

(a) Deputy Security Managers. Each department will appoint a Deputy Security Manager, in writing, with a copy to the Security Manager (Code 10) to assist the Command Security Manager in the implementation of the Information and Personnel Security Program aboard NAS Lemoore. Further delegation of Deputy

**FEB 16 2000**

Security Manager duties by departments is not authorized. Deputy Security Managers shall:

1. Perform duties of Deputy Security Manager as outlined in references (a) through (g) and this instruction.

2. Report threats to security, compromises and other security violations in writing with full details to the Security Manager for appropriate action.

3. Submit a list of those individuals, to include name, rank/rate/grade and level of clearance, authorized to receive classified material for respective departments to the Command Security Assistant (Code 10G).

4. Prepare and maintain an emergency plan that conforms with enclosure (2) and is sufficient to provide for destruction of all classified material by department in the event of an emergency.

5. Maintain a program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties for department personnel and ensure potentially significant information is reported to the Security Manager for appropriate action. Refer to Chapter 10 of reference (a) for specific guidance.

(2) Operations Security Officer. The Air Operations Officer is the Operations Security (OPSEC) Officer. The OPSEC officer supervises a program to prevent the inadvertent disclosure of any operational information that could be helpful to a potential enemy of the United States.

(3) Physical Security Officer. The Security Officer is the Physical Security Officer. The Physical Security Officer is concerned with protection of all NAS Lemoore property (including tenant activities and classified information) against theft, damage or destruction.

(4) Automated Data Processing Security Officer. The Automated Data Processing Security Officer (ADPSO) supervises a program per reference (c) to prevent damage, modification, unauthorized disclosure or loss of data or capability to process data. The ADPSO is responsible to the Security Manager for the protection of classified information being processed in an automated system, and to the Physical Security Officer for the protection of the personnel, equipment and related resources.

(5) Officers responsible for individual areas of security report to the Security Manager items relative to the security program. The Security Manager will report to the Commanding Officer on matters of security and is responsible to the Executive Officer for the administration of the Information and Security Program.

b. Security Violations. **All known or suspected security violations or compromises; all actual, potential or suspected cases of espionage, sabotage or subversions shall be reported immediately to the Security Manager.** If the Station Security Manager is unavailable, a prompt report will be made directly to the Command Duty Officer (CDO) who will report to the Security Manager any action taken. Compromise includes the loss of classified material or the exposure of classified information to unauthorized persons. The Security Manager will make notification to the Naval Criminal Investigative Service (NCIS) field office. Other matters to be reported to the Security Manager include the following:

(1) Acts of sabotage, espionage, or deliberate compromise.

(2) Contacts with citizens of communist controlled countries. Suspected counterintelligence incidents will be reported by the Security manager, via the Commanding Officer to the resident NCIS field office.

(3) Suicides or attempted suicides by anyone with access to classified material.

(4) Unauthorized absence of any personnel with access to classified material.

(5) Any safe, containing classified material, found unlocked and unattended. In the event containers or storage areas for classified matter are found open and unattended, loss or compromise of material stored therein must be presumed until an accurate determination to the contrary can be made. The container will be guarded until properly secured and investigative action will be promptly initiated in each such case.

(6) Receipt of classified material, which shows improper handling procedures by the sending activity or by NAS Lemoore personnel.

**FEB 16 2000**

a. Classification Authority and Marking. As outlined in Chapter 4 of reference (b).

6. Security Education. All personnel will receive the following security briefings and debriefings:

a. Orientation Briefing. Department Deputy Security Managers are responsible for ensuring each person who will have access to classified information receives an orientation briefing using enclosure (3) as a guideline as soon as possible after reporting aboard or being assigned to duties involving classified access. This briefing may be scheduled at regular intervals as a group orientation or given as individual instruction based on personnel turnover rate. A record of this training will be maintained by the Deputy Security Manager for possible review during command inspections.

b. On-the-Job-Training. Supervisors are responsible for ensuring subordinates are thoroughly trained on the security requirements which impact on their duty performance.

c. Refresher Briefing. Department Deputy Security Managers will ensure all personnel who have access to classified information receive a refresher briefing once a year. Topics required by paragraph 4-8 of reference (a) not otherwise being covered will be discussed. A report of the briefing will be forwarded to the Command Security Manager to include: date of briefing, department conducting the briefing, number attending and subject of training. Individual muster sheets are not desired by the Command Security Manager, but should be maintained by the Department Deputy Manager for possible review during command inspections.

d. Counterespionage Briefings. Individuals who have access to information classified Secret or above must receive a counterespionage briefing conducted by NCIS once every two years. The Command Security Manager will arrange for the counterespionage briefing with the local NCIS field office. This briefing will be scheduled twice annually. Department Deputy Security Managers will maintain musters of departmental personnel attending at their local level and forward a report of attendance including information outlined in paragraph 6c above, to the Command Security Manager. It is the Deputy Security Managers' responsibility to ensure subordinates receive this briefing at least once every two years.

e. Special Briefings. Deputy Security Managers will inform

**FEB 16 2000**

the Command Security Manager of a special briefing requirement. The Command Security Manager will coordinate the following special briefings:

(1) Foreign Travel Briefing. Individuals who have had access to classified information who plans to travel to or through a designated country (see Chapter 4, paragraph 4-10 of reference (a)) or to attend a meeting where representatives from such countries are expected to attend are required to report such plans to the Command Security Manager. This reporting requirement also applies to individuals intending cruises on Soviet ships. A defensive briefing will be coordinated with NCIS by the Command Security Manager. A debrief will be administered upon the individual's return. A record will be maintained of those given the briefing by the Security Manager for follow-up.

(2) North Atlantic Treaty Organization (NATO) Briefing. All personnel who require access to NATO information must be briefed on NATO security procedures before access may be granted.

(3) Single-Integrated Operational Plan Extremely Sensitive Information (SIOP-ESI). A special briefing is required before access to SIOP-ESI may be granted.

(4) Sensitive Compartmented Information (SCI). The Special Security Officer located at the Strike Intelligence Center, Building 004, is responsible for briefing individuals who have access to SCI.

f. Debriefings. The Command Security Manager or Command Security Assistant will provide debriefings for military personnel. The Human Resources Office will coordinate debriefings for all civilians. A sample debriefing is contained in Exhibit 4A of reference (a). The individual will then be required to read a Termination Debrief (which sets forth the provisions of the Espionage Act and other criminal statutes), read the Security Termination Statement (OPNAV Form 5511/14) and sign it. The original Security Termination Statement will be placed in the individual's official personnel record for permanent retention except at the conclusion of a Limited Access Authorization when the original will be retained in command files for two years. Individuals who have had access to classified information must be debriefed under the following conditions:

(1) Command to command transfer;

(2) Terminating active military service or civilian employment;

~~FEB 16 2000~~

(3) Temporarily separating for a period of 60 days or more, including sabbaticals and leave without pay status, or transferred to the Inactive Ready Reserves (IRR);

(4) Expiration of a Limited Access Authorization (LAA);

(5) Inadvertent substantive access to information which the individual is not eligible to receive;

(6) Security clearance eligibility revocation; or

(7) Administrative withdrawal or suspension of security clearance and SCI access eligibility for cause.

7. Accounting and Control. The Deputy Security Managers are responsible for implementing the proper accounting and control procedures specified in reference (a) and this instruction within their area of responsibility. **All NAS Lemoore personnel will strictly adhere to accounting requirements.** The Command Security Manager, Command Security Assistant and departmental Deputy Security Managers are designated control points for all incoming Secret material for the command with the exception of Special Access Program material. The Top Secret Control Office and CMS Custodian are the designated control points for all Top Secret and COMSEC material, respectively, in the command. All classified material will be under the direct control of indoctrinated, cleared personnel. Indoctrinated personnel will strictly obey all program security regulations and will maintain receipt, transfer and destruction record files (Refer to paragraph 10-19 of reference (b) for guidance).

a. Incoming Material

(1) Incoming Secret correspondence or material will be signed for and receipt cards returned to the sender. Material will be immediately entered into the NAS Lemoore control system by assigning a control number and preparing an accountability sheet using Correspondence/material Control Form (OPNAV Form 5216/10). The original of the completed control/route sheet will be forwarded to the Command Security Assistant in the Administration Department (Code 10G). The departmental Deputy Security Manager will maintain one copy on file. Secret material will not be routed as a matter of course. In lieu of this, a card or memorandum is to be routed announcing the receipt of the material and designating who to contact if access is desired.

(a) Control numbers will consist of four parts. The

first is the department initials (i.e., AD); the second a single letter (S) indicating Secret level of classification; the third, a three digit sequential serial number, (i.e., 001) and the fourth the last two digits of the current year. An example of a complete control number is: ADS00199

(2) Incoming Secret message traffic will be immediately brought under control of personnel designated and cleared to receive Secret or above material. A Secret message log will not routinely be maintained. If a Secret message is immediately destroyed upon receipt, a record of receipt is not required. If a Secret message is destroyed and witnessed by two cleared personnel a record of receipt/destruction is not required. Alternately, one person may destroy a Secret message if a record of receipt/destruction is made. However, if a Secret message will be retained, it will be recorded in the Secret message log and properly safeguarded. If a Secret message is to be retained longer than five working days, an OPNAV 5216/10 will be completed for each copy of the message, filed and distributed as defined in paragraph 7a(1) above. Elimination of Secret message destruction recording in no way diminishes the need to protect Secret messages.

(3) The Command Security Assistant will receive Secret rate training manuals from Personnel Support Activity Detachment (PSD). The Security Assistant will:

(a) Verify adequate procedures are in place to allow for storage and protected study at the requiring member's department.

(b) Assign a control number and prepare an accountability sheet.

(c) Obtain a signature from a departmental individual designated to receive classified material.

(4) Incoming confidential material will be afforded protection from unauthorized disclosure by departmental access control and compliance with procedures for marking, storage, transmission and destruction. No requirement exists to record receipt, transfer or destruction other than normal correspondence control procedures. Route slips for Confidential material are not required nor desired by NAS Lemoore.

(5) When classified material is received in a manner other than that prescribed in reference (a), a Security

**FEB 16 2000**

Discrepancy Notice (OPNAV 5511/51) will be initiated to notify the sending command of the discrepancy per reference (a). A copy of the Discrepancy Notice will be maintained by the control center receiving the material.

b. Outgoing Material

(1) All outgoing Secret material will be brought to the Command Security Assistant in the Administration Department (Code 10G) for mailing. A receipt card will be prepared for each item to be transferred out of the command. Secret material mailed out of the command will be wrapped and sent via authorized means per reference (b), paragraph 9-8.

(2) Outgoing Confidential Material. Confidential material will be wrapped and sent via authorized means per reference (b), paragraph 9-8.

c. Control of Secret Material Inside the Command. All Secret material will be kept under continuous accountability through the use of subcustody receipts. Upon signing for Secret material, the user will receive a copy of the Correspondence/Material Control Form (OPNAV 5216/10). The document will be placed in a file located in the front of the top safe drawer used to store the material. Upon return to the departmental classified material control files or to the command classified material control files, the form will be purged from the user file and the control center form will be dated in the return block. **Signatures are required for subcustody; initials are not acceptable.**

d. Reproduction of Classified Material

(1) Classified material shall be reproduced only with permission of the Command Security Manager, and only on designated equipment. The photocopier in the Commanding Officer's office in Building 700 and the photocopier in the CMS Custodian's vault in Building 004, Room 131 are designated for such reproduction. The number of copies shall be kept to a minimum, and all waste products shall be protected and destroyed as classified material. The Commanding Officer's and the CMS Custodian's photocopiers will have page 2 of enclosure (4) **prominently displayed on the equipment**. All other photocopiers will have page 1 of enclosure (4) prominently displayed on the equipment. **Reproduction of Top Secret material is prohibited.**

(2) Secret material shall be reproduced only by the

Command Security Manager, the Command Security Assistant (Code 10G), the CMS custodian, Fleet Audiovisual Facilities Pacific (FLTAVFACPAC) and the Defense Printing Service Reprographic Facility in the line of their official duties. Extra copies of Secret documents and messages shall be requested from the Command Security Assistant and not made directly by the requesting party. Copies of Confidential material may be made by the holder, subject to the general restrictions on reproduction above. Reproduced copies of classified material will be accounted for and handled in the same manner as those prescribed for the original material.

e. Control of Photography

(1) The same restrictions that apply to photocopying classified material also apply to photographic copies. All classified films, photographs, slides, and negatives, including self-processing film, shall be properly safeguarded and either marked with proper control and security markings, or destroyed as classified waste.

(2) Reference (b), paragraph 7-13 assigns discretionary authority to commanders to regulate unofficial photography. As a result, unofficial photography is generally prohibited aboard Pacific Fleet ships, stations and aircraft, even though most areas do not contain classified or sensitive material. Reference (d) changes basic Pacific Fleet security policy regarding unofficial photography of Pacific Fleet ships, stations and aircraft to permit photography (including video recording) unless there is a clear reason for not doing so. When photography is appropriately prohibited in spaces where classified/sensitive functions take place, commanders may sanitize spaces of sensitive information to permit photography of ceremonies, special events or similar unclassified activities. The following Naval Air Station Lemoore areas require access and photography restrictions and shall be so posted:

<u>Building#</u>	<u>Department/ Division</u>	<u>Work Center/ Room#</u>	<u>Restriction</u>
700	Administration	Room 205	No unauthorized access or photography unless area is sanitized.
001	Air Operations	Room 131	No unauthorized access or photography unless area is sanitized.

FEB 10 2000

005	Air Operations/ Air Traffic Control	Control Tower    No unauthorized access or photography unless area is sanitized.
-----	---	--

(3) Security entry/exit examinations are encouraged to ensure personal cameras are not introduced into areas where photography is prohibited.

f. Printing and Publishing. Prior to publication, NAS Lemoore classified publications will be handled as working papers. After the publication has been signed by the Commanding Officer and printed, all copies will be taken from the print shop to the Command Security Assistant (Code 10G) for mailing or distribution as appropriate. All working copies and master copies shall be brought under control and safeguarded appropriately. Where possible, all such material will be turned in to the Command Security Assistant (Code 10G) in the Administration Department or destroyed. After sufficient file copies have been set aside all excess copies will be destroyed.

g. Public Release Materials. All material prepared for release to the public shall be viewed by the appropriate Deputy Security Manager for inadvertent disclosure of classified information. Such information shall not be released to the public prior to review by the Command Security Manager, Station Judge Advocate or the Public Affairs Officer.

#### 8. Safeguarding and Storage of Classified Material

a. Basic Safeguarding Policy. As outlined per reference (b), Chapter 7.

b. Markings on Security Containers. As outlined per reference (b), Chapter 10.

c. Designation of Storage Sites and Restricted Areas. As outlined per reference (b), Chapter 10.

d. Securing of Classified Material. As outlined per reference (b), Chapter 7.

e. Safe Combinations. As outlined per reference (b), Chapter 10.

(1) Records of all combinations shall be sealed in a Security Container Information envelope (SF 700), marked with the appropriate classification level, and kept on file by the

**FEB 16 2000**

Security Manager (tenant) or Deputy Security Manager (NAS Lemoore departments and special assistants).

(a) If Top Secret material is involved, NAS Lemoore cannot provide storage for the combination, having no facilities suitable for that level of classification.

(b) The Deputy Security Manager and another designated holder will be responsible for maintaining the safe that contains the command's or department's safe combination envelopes. These individuals will be designated in writing, with a copy to NAS Lemoore Security Manager.

(c) For all safe combination changes, either the Deputy Security Manager or designated holder will be present in addition to the safe custodian. If the Deputy Security Manager is also the safe custodian, one other person who has access to the material will be present (i.e., department head). The Deputy Security Manager or designated holder will assume control of the Security Container Information envelope (SF 700) and will immediately place it in the safe containing the command's/department's combinations). The only official holders of the Security Container Information envelope is the Security Manager or Deputy Security Manager. This will not be delegated nor will the envelope leave the command.

(d) During safe combination changes the two representatives from the command or department will work the combination before the safe is closed.

(e) Trouble calls will not be accepted to open safes due to lost combinations unless received via either NAS Lemoore Security Manager (NAS Lemoore departments/special assistants) or COMSTRKFIGHTWINGPAC Security Manager (Type Wing and squadrons). The Public Works Officer will make the determination to drill a safe. Before contacting the Security Manager the following will be reviewed:

1. Does the safe need to be opened that day, or can it be postponed until the return of the Security Manager, designated holder, or the safe custodian?

2. Squadrons - Can information be obtained from the Type Wing or another squadron if the safe custodian is not available to access the safe?

f. Inventories/Inspections/Reviews

FEB 16 2000

(1) Top Secret. A physical inventory will be conducted by the custodian and witnessed by a properly cleared, disinterested officer at least once annually and upon change of custodian, by sight and page count. Submit a report of each inventory to the Command Security Manager.

(2) Secret. Inventory requirements for Secret material do not exist formally; however, large quantities of Secret material held by users present an opportunity for compromise. Accordingly, a Secret material turnover inventory will be conducted between the relieving custodian and the departing custodian certified by the Deputy Security Manager. The inventory will be coordinated with the Command Security Assistant (Code 10G) to ensure the command's classified inventory master route slips are signed by the relieving custodian. Submit a report of each inventory to the Command Security Manager.

(3) Internal Reviews. The Security Manager will conduct internal reviews of departments that handle classified information. This review will be conducted on a periodic, announced basis and will focus on implementation of the command's Information and Personnel Security Program at the department level. Results of the review will be provided to the department for information or action. Follow up action will be forwarded to the Command Security Manager. The Command Security Manager will maintain review results and follow up reports on file.

#### 9. Transportation of Classified Material

a. Secret and Confidential material being mailed or handcarried will be assigned NAS Lemoore control or serial numbers and will be marked with classification, declassification, page and paragraph markings as outlined per reference (b), Chapter 9.

b. Command message couriers responsible for transporting message traffic will have a Secret clearance. Couriers must present a locking briefcase to the Communications Vault in order to pickup message traffic. Message traffic will be taken directly from the Communications Vault to the receiving department. Under no circumstances will a briefcase containing traffic be left unattended in a vehicle or the trunk of a vehicle. Bulk message traffic picked up from the Communications Vault will be treated as SECRET until such time that it has been screened and the highest level of classification determined.

c. Handcarrying of Classified Material Off Station: As outlined per reference (b), Chapter 9.

10. Disposal of Classified Material

a. Destruction of Classified Material

(1) Classified material shall be destroyed as soon as it is no longer required.

(2) General destruction procedures are contained in Chapter 10 of reference (b).

(3) Burn bags containing classified material will be accounted for as follows:

(a) Burn bags for classified material no longer need to be serialized. Burn bags will be accorded the same level of protection and storage as the level of classified material they contain. Burn bags must be opaque and distinctively marked to indicate they are "burn bags". Bags must not indicate the level of classification of material to be destroyed. Bags which meet this criteria are available in the supply system

(b) All burn bags will be manifested and transported to the destruction site by two personnel cleared to the highest level of material contained in the burn bags. One of these persons must be at the E-5/GS-5 level or above. Assignment to the destruction detail will be rotated. Each department is responsible for the destruction of classified material under their control.

(4) A record of destruction is required for Top Secret information. Records of destruction are not required for classified working papers, classified waste, Confidential, or Secret information except for special types of classified information (see paragraphs 7-7 and 10-17 of reference (b)). Destruction of classified information which has been assigned an NAS Lemoore control number shall be recorded directly on the original Correspondence/Material Control form (OPNAV 5216/10) and a copy sent to the Command Security Assistant (Code 10G) in the Administration Department to ensure proper accounting.

b. Transfer of Personnel and Disposition of Classified Material

(1) Classified material is not personal property. No classified material including working papers or notes, may be taken from NAS Lemoore by detaching personnel. All personnel detaching from NAS Lemoore shall check out with the department

~~FEB 16 2000~~

Deputy Security Manager and shall return all Secret and Confidential material. A turnover inventory will be conducted by the Deputy Security Manager to ensure all classified material is present and properly receipted by the new holder. Any classified material required by an individual at his next command will be mailed following sub-paragraph 8b above.

(2) Turnover of Deputy Security Managers shall be accompanied by an inventory and inspection of the departmental classified holdings. This inventory/inspection shall be conducted by the incoming Deputy Security Manager with a written report submitted to the Command Security Manager.

c. Recovery of Classified Material Upon Death or Desertion. When any person is declared deceased or missing, classified material known to have been in his possession shall be recovered. Any material not recovered shall be reported as a possible compromise.

#### 11. Visit Control

a. Visitors. A visitor is anyone not assigned to or employed by NAS Lemoore or anyone on Temporary Assigned Duty (TAD) orders to NAS Lemoore. The movement of all visitors shall be restricted as necessary to protect classified information. Specific requirements for visitor control are outlined in Chapter 11 of reference (a).

##### b. Visit Request

(1) Prior to a visit which will involve access to classified information, a visit request must be submitted in writing to NAS Lemoore (Attention: Code 10G) by the visitor's command or home office. Visit requests may be faxed to telephone DSN 949-2856 or Commercial (559) 998-2856 if timeliness is a criteria. Hand carried visit requests will not be accepted.

(2) NAS Lemoore personnel visiting other commands must also submit specific visit requests. The Command Security Assistant (Code 10G) will prepare all visit requests for NAS Lemoore personnel visiting outside the command utilizing a naval message, letter or Visit Request form, OPNAV 5521/27.

(3) A request may be for intermittent visits over a specific period of time not greater than one year. Personnel rosters and TAD orders listing clearance held are not authorized substitutes for specific visits.

(4) Copies of all visit requests and clearance verifications submitted to NAS Lemoore will be forwarded to the department being visited and to the Security Detachment (Code 39). The Command Security Assistant (Code 10G) will maintain a file of active visit requests involving access to classified information.

c. Visits by Foreign Nationals

(1) Visits by foreign nationals, which will require the disclosure of classified information, must have the approval of the Navy International Programs Office (NAVIPO), or an authority specifically designated in reference (e).

(2) NAS Lemoore Security Detachment shall maintain a record of visits by foreign nationals or by U.S. citizens or immigrant aliens representing foreign governments, military services or private interests. These records shall be kept for two years and will include items outlined in paragraph 11-3 of reference (a).

12. Meetings. If classified information is to be disclosed at a meeting, the NAS Lemoore sponsor will ensure that:

a. Areas in which classified information is to be discussed afford adequate security against unauthorized access.

b. Adequate storage facilities are available.

c. Each person attending the classified sessions or meetings has been authorized access to information of equal or higher classification than the information to be disclosed, and that a system has been devised for positive identification of authorized attendees. Each person who is to disclose classified information has been notified of the security limitations, which must be imposed because of:

(1) The level of access authorized for all attendees.

(2) Need to know of the attendees.

(3) Physical security conditions.

d. Provisions have been made to control and safeguard classified material given to those attending and to retrieve or transfer the material through approved methods.

EFF 16 2000

e. Sessions are monitored to ensure the discussions are limited to the level authorized.

f. Notes taken of classified material are not the property of the individual but of the U.S. Navy. They must be brought under control as any classified document and transmission conducted as provided for by paragraphs 8 through 10 of this instruction.

### 13. Operations Security (OPSEC)

a. OPSEC Restrictions. The discussion of operations systems, capabilities, effectiveness, tactics, unit dispositions or changes thereto shall not be conducted over non-secure voice circuits; particularly the telephone, whether or not said information is immediately known to be classified. Neither shall any attempt be made to "talk around" classified information over the telephone.

b. OPSEC Administration. Provisions to prevent the disclosure of operational information which could be of benefit to a potential enemy of the United States shall be incorporated in all NAS Lemoore operating procedures. The OPSEC Officer shall conduct a training program to alert all NAS Lemoore members about the OPSEC threat and how to counter it.

### 14. Personnel Security

#### a. Active Duty Personnel Clearance and Access

(1) An individual's clearance must equal their access even though the security investigation may support a higher level of clearance or access. Individuals should not be allowed to use, handle or view material with classifications higher than their individual ACCESS as granted by the Commanding Officer or Command Security Manager of NAS Lemoore.

(2) Personnel generally transfer in a "no clearance" status. Upon reporting on board, the appropriate supervisor will determine if a security clearance is required and make a recommendation to the department Deputy Security Manager. The Deputy Security Manager will conduct an oral security briefing using enclosure (3), Security Orientation Briefing, as a guideline and submit a completed NAS Lemoore 5510/4 and Classified Information Non-disclosure Agreement, SF 312, (if not indicated as being previously executed) to the Command Security Manager. Following a favorably completed local records check

(i.e., legal, medical, personnel and station security, etc.) and verification of completed security investigation or submission of required security investigation requests, an interim clearance may be granted. Interim clearances granted will be documented on the member's OPNAV Form 5520/20. For military members, the original OPNAV Form 5520/20 will be maintained by the Command Security Assistant (Code 10G). If a DONCAF security clearance certification (authorizing message) accompanies the member upon transfer to this command, a final clearance is granted based upon that certification. If the member transfers to this command without a DONCAF certification, a request for final clearance authorization will be submitted to the Department of the Navy Central Adjudication Facility (DONCAF) by the Command Security Assistant utilizing OPNAV Form 5510/413. The final clearance authorization from DONCAF will be filed with the OPNAV 5520/20 maintained by the Command Security Assistant. The clearance will remain in place until the individual transfers or action is taken to downgrade or remove the clearance.

(3) Supervisors are required to regularly evaluate their personnel for continued access to classified material. Actions that may affect an individual's eligibility for access are outlined in Chapter 10 of reference (a). Managers are required to notify the Command Security Manager immediately of instances that may require an individual's continued access to classified material to be reviewed. In addition, a statement will be included in all evaluations as to the individual's continued eligibility for access to classified material.

(4) A Security Termination Statement (OPNAV Form 5511/14) will be executed upon separation, retirement or when a clearance is administratively withdrawn or revoked for cause.

(5) Access is withdrawn automatically when the individual transfers from the command, is discharged or separated from Federal Service. The Security Termination Statement is not executed upon administrative withdrawal of access alone in this instance.

b. Personnel TAD to NAS Lemoore. Personnel TAD to NAS Lemoore from other commands will not be granted access to classified information until written verification of the individual's security clearance is received by the NAS Lemoore Command Security Manager. Records of classified access given to TAD and Reserve personnel must be retained for at least two years.

**FEB 16 2000**

c. Civilian Personnel Clearance and Access. Requirements and guidance outlined in paragraph 15a above apply except as stated below:

(1) Interim clearance and access granted will be recorded on the individual's original Certificate of Personnel Security Investigation, Clearance and Access (OPNAV Form 5520/20). The original OPNAV Form 5520/20 will be maintained in the individual's Official Personnel Folder (OPF) located at the Human Resources Office with a copy maintained in command security files by the Command Security Assistant (Code 10G).

(2) Records of interim security clearances granted, as well as records of emergency access waivers of investigative requirements granted will be maintained by the Command Security Assistant (Code 10G).

(3) Final clearance authorizations from DONCAF will be filed with the OPNAV Form 5520/20 maintained by the Command Security Assistant with a copy to the employee's OPF.

(4) A civilian who is hired prior to the completion of the required personal investigation must receive a letter of emergency appointment, signed by the Command Security Manager and the Commanding Officer. Departments requesting such action must justify in writing the necessity of bringing employees on board prior to the completion of the National Agency Check and Inquiry (NACI).

(5) Department Heads. Department heads are responsible for:

(a) Determining the sensitivity of each position under his/her cognizance using the criteria outlined in reference (a) and recording this on the position description cover sheet.

(b) Ensure civilians who have been denied security clearance or have had a clearance revoked do not have access to classified material and are not assigned to, or retained in, sensitive positions.

(6) Civilian Personnel Deputy Security Manager. The Human Resources Office Director shall appoint a security assistant, designated as the Human Resources Deputy Security Manager who will be responsible for:

(a) Requesting appropriate investigations on each

**FEB 16 2000**

civilian employee and/or verifying existing security status with former employers.

(b) Transmitting correspondence concerning adverse personnel security determinations to NAS Lemoore Command Security Manager.

(c) Ensuring required security clearance documentation is filed in the official personnel folder, and investigation reports are destroyed within required time limits.

(d) Provide the original OPNAV Form 5520/20 filed in the OPF and letter of emergency appointment with supporting departmental documentation justifying emergency appointment (when applicable) to the Command Security Assistant (Code 10G) to ensure recording of command granted clearance and access.

(e) Provide proof of citizenship for civilian employees at the time a security clearance is requested.

(7) Child Development Center (CDC) Employees and Family Home Care (FHC) Providers. All individuals, regardless of employer, involved in child care services shall have completed background checks. CDCs, part-day preschool and enrichment programs, FCC providers, and contracted services shall have background checks as specified in reference (a) and Sections 10 and 32 of reference (d).

(a) Clearance and access determinations are in turn then recorded on the individual's original Certificate of Personnel Security Investigation, Clearance and Access (OPNAV Form 5520/20).

(b) Records of interim security clearances granted, as well as records of emergency access waivers of investigative requirements granted will be maintained by the Command Security Manager.

## 15. Forms

a. NAS Lemoore (112) 5510/4 Clearance Request/Authorization/Cancellation may be obtained from the Command Security Assistant, Building 700.

b. The following forms may be obtained through the supply system using the stock number listed:

(1) OPNAV 5216/10, Correspondence/Material Control (4PT), NSN 0107-LF-052-1650.

FEB 16 2000

c. Civilian Personnel Clearance and Access. Requirements and guidance outlined in paragraph 15a above apply except as stated below:

(1) Interim clearance and access granted will be recorded on the individual's original Certificate of Personnel Security Investigation, Clearance and Access (OPNAV Form 5520/20). The original OPNAV Form 5520/20 will be maintained in the individual's Official Personnel Folder (OPF) located at the Human Resources Office with a copy maintained in command security files by the Command Security Assistant (Code 10G).

(2) Records of interim security clearances granted, as well as records of emergency access waivers of investigative requirements granted will be maintained by the Command Security Assistant (Code 10G).

(3) Final clearance authorizations from DONCAF will be filed with the OPNAV Form 5520/20 maintained by the Command Security Assistant with a copy to the employee's OPF.

(4) A civilian who is hired prior to the completion of the required personal investigation must receive a letter of emergency appointment, signed by the Command Security Manager and the Commanding Officer. Departments requesting such action must justify in writing the necessity of bringing employees on board prior to the completion of the National Agency Check and Inquiry (NACI).

(5) Department Heads. Department heads are responsible for:

(a) Determining the sensitivity of each position under his/her cognizance using the criteria outlined in reference (a) and recording this on the position description cover sheet.

(b) Ensure civilians who have been denied security clearance or have had a clearance revoked do not have access to classified material and are not assigned to, or retained in, sensitive positions.

(6) Civilian Personnel Deputy Security Manager. The Human Resources Office Director shall appoint a security assistant, designated as the Human Resources Deputy Security Manager who will be responsible for:

(a) Requesting appropriate investigations on each

civilian employee and/or verifying existing security status with former employers.

(b) Transmitting correspondence concerning adverse personnel security determinations to NAS Lemoore Command Security Manager.

(c) Ensuring required security clearance documentation is filed in the official personnel folder, and investigation reports are destroyed within required time limits.

(d) Provide the original OPNAV Form 5520/20 filed in the OPF and letter of emergency appointment with supporting departmental documentation justifying emergency appointment (when applicable) to the Command Security Assistant (Code 10G) to ensure recording of command granted clearance and access.

(e) Provide proof of citizenship for civilian employees at the time a security clearance is requested.

(7) Child Development Center (CDC) Employees and Family Home Care (FHC) Providers. All individuals, regardless of employer, involved in child care services shall have completed background checks. CDCs, part-day preschool and enrichment programs, FCC providers, and contracted services shall have background checks as specified in reference (a) and Sections 10 and 32 of reference (d).

(a) Clearance and access determinations are in turn then recorded on the individual's original Certificate of Personnel Security Investigation, Clearance and Access (OPNAV Form 5520/20).

(b) Records of interim security clearances granted, as well as records of emergency access waivers of investigative requirements granted will be maintained by the Command Security Manager.

## 15. Forms

a. NAS Lemoore (112) 5510/4 Clearance Request/Authorization/Cancellation may be obtained from the Command Security Assistant, Building 700.

b. The following forms may be obtained through the supply system using the stock number listed:

(1) OPNAV 5216/10, Correspondence/Material Control (4PT), NSN 0107-LF-052-1650.

NASLEMINST 5511.2M

FEB 16 2000

(2) OPNAV 5510/413, Personnel Security Action Request, NSN 0107-LF-009-4200.

(3) OPNAV 5511/14, Security Termination Statement, NSN 0107-LF-055-1171.

(4) OPNAV 5511/51, Security Discrepancy Notice, NSN 0107-LF-055-5355.

(5) OPNAV 5520/20, Certificate of Personnel Security Investigation, Clearance, and Access, NSN 0107-LF-055-2101.

(6) OPNAV 5521/27, Visit Request, NSN 0107-LF-055-2235.

(7) Standard Form 312, Classified Material Non-disclosure Agreement, NSN 7540-01-280-5499.

(8) Standard Form 700, Security Container Information, NSN 7540-01-214-5372.

(9) Standard Form 701, Activity Security Checklist, NSN 7540-01-213-7899.

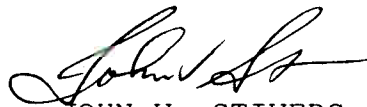
(10) Standard Form 702, Security Container Check Sheet, NSN 7540-01-213-7900

(11) Standard Form 703, Top Secret Cover Sheet, NSN 740-01-213-7901.

(12) Standard Form 704 Secret Cover Sheet, NSN 7540-01-213-7902.

(13) Standard Form 705, Confidential Cover Sheet, NSN 7540-01-213-7903.

(14) DD Form 2501, DOD Courier Card, NSN 0102-LF-000-6900.



JOHN V. STIVERS

Distribution: (NASLEMINST 5215.2W)  
List A

**FEB 16 2000**Classified Material Storage Site Listing

<u>Department</u>	<u>Storage Bldg#</u>	<u>Site/ Room#</u>	<u>Safe#</u>	<u>Responsible Personnel</u>
Administration	700	220	L2006	Security Assistant
	700	205	30989B	Commanding Officer
Air Operations	001	102	L998	AO Deputy Security Mgr.
	001	133	L534	GEMD Officer
AIS	773	Gateguard	L702	AIS Deputy Security Mgr.
	773	Warehouse	1464111	AIS Deputy Security Mgr.
CMS	004	131	L533	CMS Custodian
	004	131	1575076	CMS Custodian
	004	131	1210529	CMS Custodian
	004	Vault	L130	CMS Custodian
	004	Vault	L131	CMS Custodian
	140	Vault	L405	CMS Custodian
Public Works	750	104	L819	PW Deputy Security Mgr.
Security	705	Admin Office	1260296	Security Deputy Security Mgr.
Supply	140	Mat'l Div Vault	L404	Supply Deputy Security Mgr.
	140	Tech Branch	L194	Supply Deputy Security Mgr.
	773	Resource Management Branch	1220955	Supply Deputy Security Mgr.

~~FEB 16 2000~~Classified Material Storage Site Listing

<u>Department</u>	<u>Storage Bldg#</u>	<u>Site/ Room#</u>	<u>Safe#</u>	<u>Responsible Personnel</u>
Weapons	440	Armory	L629	Weapons Deputy Security Mgr.
	440	Armory/ Vault	1027	Weapons Deputy Security Mgr.
	440	AWO	L95	Weapons Deputy Security Mgr.
	440	Armory/ Vault	L626	Weapons Deputy Security Mgr.
	440	Armory	L970	Weapons Deputy Security Mgr.
	440	Armory	L527	Weapons Deputy Security Mgr.
	420	Magazines	Key	Weapons Deputy Security Mgr.
	472	Missiles	Key	Weapons Deputy Security Mgr.
	440	Armory	L1032	Weapons Deputy Security Mgr.
	440	Armory	L1033	Weapons Deputy Security Mgr.
	440	Armory/ Vault	L1034	Weapons Deputy Security Mgr.
	440	Armory/ Vault	L1035	Weapons Deputy Security Mgr.
	440	Armory	Key	Weapons Deputy Security Mgr.
	440	Armory	L892	Weapons Deputy Security Mgr.
	472	Missiles/ Vault	L640	Weapons Deputy Security Mgr.

### Emergency Plan

1. Purpose. This Emergency Plan establishes procedures and responsibilities for the protection and possible destruction of classified material in the case of an emergency.

2. Implementation. Implementation of this Emergency Plan will be ordered by the Commanding Officer, Executive Officer, the Security Manager, or the OPSEC Officer, when directed by higher authority or when an emergency justifying such action is judged to exist.

3. Location. Storage locations for classified material are listed in enclosure (1) of this instruction.

4. Destruction. Classified material shall be destroyed in the following priority:

- a. CMS keying material and equipment.
- b. Top Secret material and equipment.
- c. Secret documents, messages and other material and equipment.
- d. Confidential material and equipment.

Destruction will be supervised by the persons indicated in paragraph 2 or by individual safe/storage site custodians; or in their absence, by designees of the Security Manager or Deputy Security Managers. Given sufficient lead time, destruction will be by department shredding machine (Machine must meet the requirements per reference (a) (OPNAVINST 5510.1H)). Emergency destruction at storage sites, when necessary, will be accomplished by burning in waste barrels covered with screening. The fires shall be started outside the local buildings in a position which will minimize danger to personnel, aircraft or equipment. Classified CMS keying equipment shall be destroyed by mutilation with hammers, axes, or other heavy tools. All classified equipment will be destroyed as CMS keying equipment.

### 5. Action

a. In emergencies that require protection rather than destruction of classified material, members of the duty section or Security Detachment may be used to form a protective perimeter around the storage site. Such a perimeter will provide adequate

FEB 16 2009

protection rather than stationing individual guards by each safe inside the storage site. Duty section members shall be briefed in the annual security refresher brief to stop unauthorized persons from entering the storage site and from removing classified material.

b. The Deputy Security Manager is responsible for providing on a quarterly basis (or sooner if change of personnel occurs) their duty and home phone numbers, the responsible users' duty and home phone numbers and the location and number of the safe holding all the department's combinations. The Security Manager will provide this list to the CDO. In the event of an emergency destruction either the Security Manager or the CDO will contact either the Deputy Security Manager or responsible user to inform them of the required actions. The Deputy Security Manager will maintain a roster of safe custodians with their duty and home phone numbers. This roster will be used to recall personnel to aid in the emergency destruction of the material.

SECURITY ORIENTATION BRIEFING

- Explain the purpose of the briefing.
- Explain clearance and access in general terms.
- Explain the individual's clearance and access.
- Discuss need-to-know.
- Telephone Security (TELSEC).
- Handling procedures for classified material during working hours.
- Clean desk policy at close of business is best and the most secure procedure.
- Check sheets should be used to assist in checking:
  - Classified material is properly stored.
  - Burn bags have been picked up.
  - Safes are locked and double checked.
  - Doors and windows are secured.
  - Classified waste is properly secured.
  - Classified material has not been placed in waste containers.
  - Your desk and the desks of others in your work area are clear, and there is no classified material adrift.
  - After hours security checks.
- Security of classified message traffic is a problem due to the volume handled.
- Discuss marking outside (top and bottom, front and back) of all folders or binders with the highest classification of information contained therein.
- Discuss marking working papers with appropriate classification.
- Discuss authorized storage facilities.

FEB 16 2000

- Desk drawers are not authorized for overnight storage and should never be used, even for temporary daytime storage.
- GSA approved security containers with built-in combination locks should be used for storage of classified material.
- Designated file cabinets with welded bars and combination locks should be used for storage of Confidential material only.
- Use of reproductive machines for reproduction of Top Secret material and all classified material covered by special access programs and/or marked with special dissemination and reproduction limitations is prohibited.
- Discuss common discrepancies.
- Discuss security of the building.
- Provide names of security personnel for the command.
- Discuss classified visits.
- Proper passing of clearance data.
- Never carry safe combinations in wallets or purses.
- Hostile intelligence threat in area.
- Procedures to be followed in the event one suspects he has been contacted by a hostile collector.
- Approaches used by hostile human intelligence collectors.
- Discuss the proper procedures and command policy for handcarrying classified material.
- Discuss the requirement to report to the Command Security Manager any proposed personal foreign travel prior to commencing such travel.
- The Security Manager is responsible for the successful administration of the command's security program. The Security Manager can only be effective through the conscientious assistance of all hands.

**This Copying Machine**

**may be used for reproduction**

**of UNCLASSIFIED material ONLY.**

**Reproduction of classified “MUST BE”**

**APPROVED BY**

**Security Manager**

**Room 226, Ext 2739**

**This Copying Machine**  
  
**may be used for reproduction**  
  
**of material up to SECRET.**

**Reproduction of classified “MUST BE”**

**APPROVED BY**

**Security Manager**

**Room 226, Ext 2739**